

Express Mail Label Number: EL919127904US

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
APPLICATION FOR UNITED STATES PATENT**

**TITLE: SEMICONDUCTOR QUANTUM CRYPTOGRAPHIC DEVICE
AND METHOD**

INVENTORS: Matthew J. Gilbert
David K. Ferry

Attorneys: Thomas D. MacBlain
Gallagher & Kennedy, P.A.
2575 East Camelback Road
Phoenix, Arizona 85016-9225
Telephone: (602) 530-8088

SEMICONDUCTOR QUANTUM CRYPTOGRAPHIC DEVICE AND METHOD

Related Applications

This application claims priority from provisional United States patent application serial No. 60/400,969, filed August 2, 2002, entitled Semiconductor Quantum Cryptographic Device and Method, in the names of Matthew J. Gilbert and David K. Ferry. That application is 5 incorporated herein by reference.

This application is related to Patent Cooperation Treaty (PCT) application filed on behalf of the Arizona Board of Regents, as applicant, having the same title as this application, filed concurrently herewith and claiming priority from the same, above-identified U.S. provisional 10 application.

Statement of Government Funding

Financial assistance for this project was provided by the U.S. Government through the Office of Naval Research under Grant Number N00014-01-1-0741/SC No. 10-6387-1 and the United States Government may own certain rights to this invention.

15 Field of The Invention

This invention relates to quantum gate devices useful for quantum computing and in encrypting of quantum computer generated messages.

Background

Recently, quantum computing has received a great deal of focus as a means for replacing 20 the traditional complementary metal-oxide-semiconductor architecture. This has been, in large part, due to the numerous attractive features that quantum computing offers. Of these features, the most popular is the ability to achieve very rapid computation speeds as compared with that of the classical computation. However, in addition to simply being a method to speed the computation, quantum computing offers tremendous promise in areas that are classically 25 unrealizable or impractical, such as quantum teleportation and the factorization of very large numbers into requisite primes. If realized, the latter ability, which exploits the massive

parallelism of quantum computation, would render all of the current public codes vulnerable to eavesdropping.

Quantum computation theory has been structured around the use of a qubit, or quantum bit. Two or more bits of quantum information are coupled together to achieve basic logic structures whereby the most basic and essential coupling of two qubits is the controlled not gate (CNOT). One popular realization of this gate is in the Fredkin Gate. E. Fredkin and T. Toffoli, 21 *Int. J. Theor. Phys.* 219 (1982). The Fredkin gate consists of a control bit, coupled to a qubit, and it operates on the following principle: if a "1" is present in the control bit, then the qubit is passed unchanged. On the other hand, if a "0" is present in the control bit, then the qubit is inverted.

There have been several implementations offered to solve the problem of quantum hacking, but the majority of these implementations have either revolved around the use of differing polarizations of photons or used nuclear magnetic resonance to transmit bits based on different quantum keys, or protocols. The ability to implement a cryptographical system in a solid-state setting has not been offered previously. The ability to encrypt transmissions in a semiconductor setting would enable the cryptography scheme to be integrated into existing semiconductor chips to provide secure transmissions of data.

Brief Summary

In a first aspect of the invention a quantum semiconductor gate is provided. Turning on and off a bias causes the gate output to appear at one or another of the gate outputs. The gate has a pair of waveguides. An input section of at least one of the waveguides leads to a coupling region, where, by tunneling, the two waveguides are coupled. An output section of each of the waveguides leads from the coupling section to an output end of the waveguide. The length of the coupling ordinarily will determine at which of the two waveguide outputs charge carriers (typically electron) moving into the coupling will appear. A biasing element, if activated, causes carriers moving through the input section of the one waveguide into the coupling region to be coupled to the output section of one or the other of the waveguides. An on and off condition of the bias, then, can be considered an input "1" and "0" respectively. At the waveguide outputs, presence of current carrier density can be considered a "1" or high condition and absence of

carrier density can be considered a "0" or low condition. Without more, this device can serve as a logic gate for quantum computing.

The biasing element that directs the current carrier density to either the first or the second waveguide output can be either an electrical bias applied across the device or a magnetic bias applied thereto.

5 The gate can be implemented in a GaAs/AlGaAs heterostructure, although for the cryptographic application described below, an InGaAs/InAs heterostructure is preferred.

Semiconductor device fabrication techniques are used to provide the pair of generally parallel electron waveguides. These are separated at their ends by potentials applied to the 10 semiconductor in which the carriers move by a pair of deposited conductor metal members, called variously gates or barriers. The gates and further metal deposits formed along the device in the direction of wave propagation provide the potentials that bound the waveguides. The deposited metal elements are electrically biased to present the potential barriers. One of the waveguides is of uniform width, i.e. has the same width at both of its ends. The other waveguide 15 is wider at the output side of the device. The two metallic members project toward each other from the input and output ends of the device. The potential barriers that they produce are separated by a tunnel region that forms a coupling where the two waveguides are coupled at their middles so as to permit controlled charge carrier density relocation from one waveguide to the other.

20 Influencing a flow of electrons by application of a magnetic field to control electron density location in a pair of waveguides coupled at a slot that communicates between them has been reported. J. Harris, R. Akis and D. K. Ferry, *Magnetically switched quantum waveguide qubit*, 79 App. Phy. Lett. 2214 (2001), incorporated herein by reference. In M. J. Gilbert, R. Akis and D. K. Ferry, *Dual computational basis qubit in semiconductor heterostructures*, 83 App. 25 Phys. Lett. 1, (2003), incorporated herein by reference, the inventors report simulation of the device of this invention for the purpose of secure encryption.

The inventors have shown that, as here, two waveguides coupled centrally at a tunnel region can be controlled by application of an electrical bias as well as by a magnetic field to effect electron density transfer from one waveguide to the other. M. J. Gilbert, R. Akis and D. 30 K. Ferry, *Magnetically and electrically tunable semiconductor quantum waveguide inverter*, 81 App. Phys. Lett. 4284 (2003), incorporated herein by reference.

The dimensions contemplated are very small, but are susceptible of scaling up. The first waveguide is about 35 nm wide, the coupling region is 300 to 450 nm long, preferably 335 nm. The input region of the second waveguide is narrow, about 20 nm wide and the output region is wide, about 45 nm wide to assure coupling of the electron density under influence of the bias and

5 without decay.

Built onto the conceptual basis of the gate just described, a semiconductor device or qubit possessing two separate computational bases is provided as a means of circumventing the problem of quantum hacking. The device accomplishes bit encoding both through the control of the location of charge carrier (electron) density and by manipulation of the spin of those charge

10 carriers. This is implemented, in a preferred, exemplary embodiment in an InGaAs/InAs heterostructure that uses a coupled electron wave guide structure with an imbedded quantum point contact. A magnetic or electrical bias is controlled to encode the location of electron density and the application of a magnetic field at the location of a quantum point contact is controlled to manipulate electron spin. The control of electron density location and spin affords

15 two controllable, nonorthogonal features that can be communicated. This enables the implementation of known cryptography techniques to provide bit encoding that is secure against eavesdropping. C. H. Bennett, *Quantum cryptography using any two nonorthogonal states*, 68 Phys. Rev. Lett. 3121 (1992), incorporated herein by reference, and C. H. Bennet and G. Brassard, *Proceedings of IEEE Int. Conf. on Computer Systems, and Signal Processing*,

20 Bangalore, India (IEEE, New York, 1984), p. 178, incorporated herein by reference.

Use of a quantum point contact in the presence of a magnetic field to filter electron spin has been shown. See, e.g. M. J. Gilbert and J. P. Bird, *Application of split-gate structures as tunable spin filters*, 77 App. Phys. Lett. 1050 (2000), incorporated herein by reference. Here, in a quantum gate device of the kind described above, the quantum point contact is used in this

25 manner to filter (i.e. polarize) the spin of electrons moving in a first of the waveguides by Zeeman splitting. Application and removal of the magnetic field toggles the electron current in the waveguide between spin polarized and nonpolarized.

In the preferred embodiment described here, the charge carriers are electrons. It is nevertheless conceivable that the apparatus and method of the invention can employ charge

30 carriers other than electrons, ions for example, that are susceptible to having the spin state of their electrons polarized. Also as described with respect to the exemplary preferred embodiment,

application of the electrical or magnetic bias that controls the location of the carrier current at the device's output causes the carrier current to switch from a first waveguide to the output section of a second waveguide. However, it is the length of the coupling tunnel region that determines which waveguide's output section will ordinarily receive the carrier density. So, clearly, the 5 electrical or magnetic bias can be applied to cause the carrier density to appear at the output of the originating waveguide where the coupling length is such as to ordinarily result in the carrier density appearing at the output of the second waveguide rather than the originating waveguide output.

10 The above and further objects and advantages of the invention will be better understood from the following detailed description of at least one preferred embodiment of the invention, taken in consideration with the accompanying drawings.

Brief Description of the Drawings

15 Fig. 1 is a schematic, functional block diagram and shows an exemplary connection of a device of the present invention with sources of electron flow, bias voltages and magnetic field-producing currents;

Fig. 2 is a diagrammatic illustration, not to scale, showing the dimensions of the device of Fig. 1;

Fig. 3 is a plot of the potential barriers at boundaries of waveguides of the device of Figs. 1 and 2;

20 Fig. 4 is a pair of graphs plotting (a) the individual transmissions (T11 and T12) plotted over the coupling length between the two waveguides of the device of Figs. 1 and 2, and (b) total transmission and reflection plotted over the coupling length between the two waveguides;

Fig. 5 is a series of graphs of (a) density at zero magnetic field with the coupling length f of Fig. 2 set to 335 nm, (b) density with a 0.705T magnetic field applied to the structure of the 25 device of Figs. 1 and 2, (c) transmissions T12 and T11 plotted over a varying magnetic field, and (d) the total transmission and reflection plotted over a varying magnetic field;

Fig. 6 is a series of graphs of (a) density with zero applied bias at a 335 nm coupling length, (b) density with 0.73meV applied bias, (c) density with 0.94meV applied bias, and (d) individual currents (I11 and I12) plotted against a varying applied bias of 0-2meV;

Fig. 7 is a two dimension depiction of the structure of the device of the invention;;

Fig. 8 is a series of graphical representations of the effects of electrical bias on the device of Fig. 1 - 3 and 8, (a) showing electron density distribution at a first bias, (b) showing density distribution at a second bias, (c) plotting currents against varying electrical bias, and (d) plotting 5 total current against varying bias;

Fig. 9 is a series of plots of operation of the spin polarizing features of the invention including (a) showing probability varying with energy and magnetic field, (b) showing current varying with energy and magnetic field, (c) plotting current vs. time, and (d) magnetic field vs. time; and

10 Fig. 10 is a series of plots of vs. time of (a) variable a controlling output location, (b) random variable b controlling spin polarization, (c) current flowing to the output of the input waveguide (I11), and (d) current to the output of output waveguide (I12).

Detailed Description

As shown in Fig. 1, a semiconductor logic component 20 has a deposited metal strip 22 15 that has a potential established by a suitable source of potential shown in Fig. 1 as the voltage source 24. By the potential boundary that it produces in the semiconductor on which it is deposited, the conductive metal strip 22 forms a first, continuous boundary of a first, "input" waveguide 26. A conductive metal member 28 similarly forms a second boundary of the waveguide 26 at the left, input end of the device 20. Again a suitable potential is applied to the 20 member or gate 28 by the voltage source 24. At its further, output end, the waveguide 26 is bounded by the potential afforded by another deposited conductive metal member 30. To this end, this gate 30 is, again, provided a potential as schematically indicated by its connection to the voltage source 24. The waveguide 26 is of uniform width. Fig. 3 plots the potential barriers formed at the metallic strips 22 and 34 and at the two metal members 28 and 30. In the 25 exemplary embodiment described, each potential boundary is slightly greater than 0.2 eV.

The potentials from the members 28 and 30 stand as barriers that isolate the input waveguide 26 from a further, output waveguide 32. The waveguide 32 is bound by the potentials from the two members 28 and 30 and from a further deposited conductive metal strip 34. A potential is applied to the metal strip 34 as indicated schematically by its connection to the 30 voltage source 24. The second, output waveguide 32 is narrower at its left, input end 31 and

wider at its right, output end 33 by virtue of the member 30 being narrower than the member 28. The output end of the waveguide 32 is, in fact, wider than the first, input waveguide 26.

Intermediate the potential boundaries of the two gates 28 and 30 lies a tunnel region 36. This tunnel region 36 serves as a coupling between the two waveguides 26 and 32. However, 5 without some biasing influence, in this particular exemplary embodiment, electrons (the charge carriers) introduced at the input end of the first, input waveguide 26 will move through that waveguide to its output end.

Turning to Fig. 2, the actual dimensions of a preferred, exemplary embodiment of the logic device are as follows:

10	width <u>a</u> of waveguide 26	- 35 nm
	width <u>b</u> of waveguide 32 at its input end	- 25 nm
	width <u>c</u> of waveguide 32 at its output end	- 45 nm
	length <u>d</u> of the gate 28	- 100 to 150 nm
	length <u>e</u> of the gate 30	- 100 to 150 nm
15	length <u>f</u> of the tunnel region 36	- 335 nm
	width <u>g</u> of the gate 28	- 50 nm
	width <u>h</u> of the gate 30	- 25 nm

Returning to Fig. 1, a source of electron flow 40 introduces electrons into (or causes carrier flow within) the input end of the input waveguide 26. Electrons move toward the tunnel 20 region 36. There is provided a controlled source of bias. This may be electrical. Schematically, for purposes of explanation, a biasing element shown as a potential bearing screen allowing electrons to pass, while presenting a biasing potential with a plate or drain 44, connected to the voltage source 46 through a switch 48. Alternatively, as discussed further below, the bias may be magnetic, as schematically indicated in broken lines in Fig. 1 as the coil 52 connected to a 25 current source 54 via a switch 56.

As thus far described, the device is a controlled NOT (CNOT) gate and can be used in quantum or nanostructure binary computer installations as such. Lack of a bias, or a low level bias, at the tunnel region 36, represented by an open switch condition of switch 48 or 56, can be considered, for example, a "0" input. Electron density will appear at the output side of the input 30 waveguide 26 (a "1" or "high" output). At the output side of the output waveguide 32 no electron density will appear (a "0" or "low" output). Application of a bias by closure of switch

48 or switch 52 may be considered an input "1." The output side of the output waveguide 32 now is coupled via the tunnel region 36 to the input side of the input waveguide 26. Electron density is removed from the output side of the input waveguide ("0" or "low") and appears at the output side of the output waveguide ("1" or "high"). A first controlled computational basis has 5 thus been provided.

At the input side of the input waveguide 26 of the device 20 in Fig. 1, there is provided a quantum point contact (QPC) 60. A magnetic field source 64, schematically shown as a coil, is connected via a switch 66 with a current source 68.

In this instance device 20 is preferably an InGaAs/InAs heterostructure. InAs is used as 10 the semiconductor of choice due to the enhanced Landé g-factor that InAs possesses, - 15, as compared with more popular semiconductors such as GaAs, which has a g-factor of only -0.44. This allows filtering the electron spins with a reduced magnetic field.

In the absence of a magnetic field, the electron density introduced by the electron current source 40 will be without spin polarization. Upon application of the magnetic field the electrons 15 at the quantum point contact will be polarized with either an up spin or a down spin depending on the direction (sign) of the magnetic field applied. This, then, gives a second, controlled, computation basis, i.e. spin-polarized electron density appearing at the output side of the device 20 or electron density without spin polarization appearing at the output side of the device. The two bases for computation-spin polarization or not and electron appearance in one or the other of 20 the waveguides - are nonorthogonal computational bases. In known fashion, then, encryption of communications can be accomplished between the input side and the output side of the device 20, including the secure determination of encryption keys usable for encryption by the sender, who controls the spin and output coupling, and also usable for decryption by the receiver.

Although, in Figs. 1 - 3, the device 20 has been represented as a stand-alone device for 25 purposes of explanation, it will be understood that such devices can be part of an integrated circuit formed on a single chip. Also the use of individual voltage sources and current sources in Fig. 1 is for purposes of explanation only. Typically bias voltages and current available in an integrated circuit are available for use in known fashion to afford the needed potentials and electrical current. Magnetic field generation has been illustrated as being through the use of a 30 coil whereas in integrated circuitry a single wire or deposited lead may be used in proximity to

the device 20 to provide the desired magnetic field for spin polarization and for magnetic bias across the device in the tunnel region.

In Fig. 3, to stimulate more realistically the potential profile for the barrier potentials, at the metallic barrier members 28 and 30, the initial "hardwall" potential has been smoothed with a 5 Gaussian distribution. The potential barrier, however, is still sufficiently high to prevent any leakage from the input waveguide to the output waveguide and to assure that all transfer of electron density from the input to the output occurs in the tunnel region 36.

The wider output region 33 of the output waveguide 32 assures that modes propagate through the coupling region and do not decay. The substrate of the device is doped to set the 10 Fermi level. The Fermi energy in the structure is chosen to be 2 meV, which corresponds to a carrier density of $5.6 \times 10^{10} \text{ cm}^{-2}$. This Fermi energy is chosen so that only one mode is excited in the input waveguide of the structure. Since the input waveguide structure is wider than the output waveguide structure at the input thereof, the mode that is excited at this energy will only propagate in the wider input waveguide. The particular dimensions of the waveguide structure 15 can be easily scaled as long as the constraints mentioned are honored.

The density in the structure for varying coupling lengths is calculated to find the maximum output, which occurs at the peak in the coupling of the wavefunction from the input waveguide to the output waveguide. The results of a simulation are shown in Fig. 4. In Fig. 4(a) there are periodic fluctuations in transmission from the input waveguide to the output of the 20 second waveguide 32 (such transmissions are designated here as T12), and from the input waveguide 26 to the output of the initial waveguide 26 (such transmissions are, here, T11). These fluctuations are periodic in coupling length at approximately 300 nm. Every 150 nm is an almost "pure" state ($|0\rangle$ or $|1\rangle$). Other coupling lengths are at intermediate locations on the 25 Bloch sphere and thus one finds superposition states. For the device of Figs. 1 - 3, a coupling length of about 335 nm results in a maximum $T_{11} = 0.90626$ and a minimum $T_{12} = 0.0303$ resulting in an almost pure state. Fig. 4 (b) plots the total transmission and total reflection against the coupling length. There remains a reflected component of 0.0671 at the optimum coupling length which accounts for the remainder of the density.

With a coupling length selected, various magnetic fields are applied and the resulting 30 densities in the input waveguide 26 and the output waveguide 32 are plotted in Fig. 5. Fig 5 (a) plots the density with no magnetic field. As before, the majority of the density remains in the

input waveguide 26 output or "cathode" section, maximizing transmission T11. As seen in Fig. 5 (b), with a magnetic field of 0.705 T, the wavefunction is transferred from the input waveguide 26 input side (or anode) to the output waveguide 32 output side (or cathode) via the tunnel region 36 and a "pure" inverted state in the system is achieved, maximizing T12. From Fig. 5 (c), T12
5 is approximately 0.983, T11 is approximately 3.451×10^{-5} , and the total reflection is approximately 0.0171. While T11 is greater than zero, the value of this transmission is negligible compared to T12, which can be regarded as a "pure" state. Furthermore, from Fig. 3 (d) it can be observed that the application of a magnetic field is a symmetric process in total transmission and reflection, but is not for the individual transmissions of the input and output
10 waveguides (T11 and T12) individually. Minima of transmission occur at half-integer multiples of the cyclotron radii compared to the corresponding coupling length of the structure. Based on these results, it is determined that using this coupled waveguide structure a small magnetic field of 0.705 T will switch the outputs represented by the two waveguide output sides from a "low" to a "high" or "high" to "low" state.

15 While it is clear that the output of the coupled waveguide structure may be switched using a magnetic field, it is not clear that the application of a magnetic field is always the most efficient way to switch a quantum gate or qubit. In one exemplary embodiment the application of the magnetic field comes from the bias of a very thin wire affixed to the surface of the semiconductor. While the application of a magnetic field through the use of a small wire may be
20 acceptable in the case of a single gate, magnetic switching may not be feasible in the case of a multiple gate structure. With the gate structures packed very tightly in the semiconductor structure, conceivably, many wires could be needed to switch the various individual gates. While it is possible to pack the gates tightly, it may very well not be possible to adequately control the current in the wires needed to switch the states of the individual gates. When the
25 wires are brought into close proximity of each other, the magnetic fields of the individual wires will likely interfere and the result would be a shift in the magnitude of the magnetic field that the gates would see. This could result in an ineffective switching of the state of the gate. The effect is illustrated in Fig. 5 (c), where the plateau is not terribly stable as small changes in the magnitude of the magnetic field produce a superposition state.

30 Therefore, in certain embodiments it is preferable to seek a means by which the state of the gate may be changed through the application of an applied electrical bias. This case is

considered to be better where multiple gates are densely packed as the electrical bias may be applied in a much more localized fashion than the magnetic field.

Fig. 6 plots the results of adding a voltage drop, ranging from 0 to -1.25 mV across the coupled waveguide structure of device 20. This adds an extra degree of freedom to the carriers in the system, and it is no longer viable to discuss the operation of the device in terms of just the transmissions and reflections of incident modes. The addition of an extra degree of freedom to the carriers excites extra output modes which are indistinguishable in the total transmission from the initially excited mode (determined by the setting of the Fermi energy). Therefore, in order to determine the extent to which this device switches from one pure state to the next, the Landauer formula is used to integrate over the individual transmissions and compute the current. Fig 6 (a) shows the density plotted with no applied bias at the T11 maximum. As expected, the plot is identical to Fig. 5 (a). A negative bias is now applied (applied uniformly from the source at the left end to the drain at the right end) across the device. The resulting density change is shown in Figs. 6 (b) and 6 (c) for applied biases of -0.243 mV and -0.318 mV respectively. While it is clear from Figs. 6(b) and 6 (c) that the majority of the density has switched and is now propagating at the output waveguide 32 output end (cathode), the current flowing in each waveguide 26 and 32 must be looked at to determine the level of success in switching of the waveguide states. In Fig. 6 (d), in the case of both the -0.243 mV and -0.318 mV applied biases, no current is flowing in the input waveguide output or cathode (I11) and a vast majority of the current flowing is in the output waveguide 32 output or cathode (I12), thereby giving a switched state. The magnitudes of the currents flowing at these applied biases are -46 nA at -0.243 mV applied bias and -40 nA at -0.318 mV. Further, in both cases the total current, and the current that is flowing at the input or anode end of the output waveguide 32, are equal. Thus, the switching from one pure state to another is complete as the applied bias is increased. Moreover, in Fig. 6 (d) the current in the device pinches off at -0.6 mV. This is expected, as when the applied negative bias increases, the Fermi level at the input or anode end of the structure eventually drops below a point in energy where propagating modes can be supported in the structure. Therefore, the device pinches off.

A simulation of this system has performed on a discretized grid using a variation of the 30 Usuki mode matching technique via the scattering matrix, using a grid spacing of 5 nm. The

simulation of the system was kept as realistic as possible. To this end, thermal effects and Zeeman splitting into the system were included.

Fig. 7 is a two dimensional profile of the structure used in a simulation of the device of the invention. In this figure, the corresponding operational sections of the system are labeled.

5 The first section is the input section which contains the quantum point contact (QPC) and extends to the end of the potential barrier. It is here that the incoming mode is polarized (or not) by the local magnetic field in the QPC. Further, the public section contains the tunnel region. In this section, the mode interacts with the output waveguide and, based on an input electrical bias, selects an output waveguide. Finally, the output region is shown where the receiver makes

10 measurements.

The effects of electrical bias are illustrated in Fig. 8. In Fig. 8 (a) is shown electron density when the electrical bias is $V_{sd} = -0.78$ mV with $T = 0.7$ K. This corresponds to a maximal current in the transmitted current present in the input waveguide ($|11\rangle$). In Fig. 8 (b), electron density is shown when the electrical bias is $V_{sd} = -1.64$ mV with $T = 0.7$ K. This corresponds to a maximal current in the output waveguide ($|12\rangle$). Fig. 8 (c) plots $|11\rangle$ and $|12\rangle$ against a varying electrical bias to show the profile of the individual transmissions. In Fig. 8 (d), total current flowing in the device is plotted against a varying electrical bias to show the profile of the total transmission through the device.

15 Fig. 9 illustrates the operation of the quantum point contact as a spin filter. Fig. 9 (a) is a surface plot of the absolute transmission probability ($T_{abs} = T_{\downarrow} - T_{\uparrow}$) for a QPC of potential profile $V(x, y) = V_0 - \frac{1}{2} m \cdot \omega_x^2 x^2 + \frac{1}{2} m \cdot \omega_y^2 y^2$ with $V_0 = 8.0$ meV, $\hbar\omega_x = 0.1$ meV, $\hbar\omega_y = 0.05$ meV, and $T = 0.7$ K with varying energy and magnetic field. Fig. 9 (b) is a surface plot of the polarization ($P = \underline{T_{\downarrow}} - \underline{T_{\uparrow}}$) of the incoming electrons plotted against varying energy and

$$T_{\downarrow} + T_{\uparrow}$$

20 magnetic field. Fig. 9 (c) plots filtration characteristics for electrons with incident energy corresponding to $V_{sd} = -0.78$ mV. And Fig. 9 (d) plots filtration characteristics for electrons with incident energy corresponding to $V_{sd} = -1.64$ mV.

25 Fig. 9 illustrated simulated operation of the cryptographical device 20. Fig. 9 (a) plots the random variable a which controls the ultimate location of the electron density as a function of time. Fig. 9 (b) plots the random variable b which controls the polarization of the electron density as a function of time. Fig. 9 (c) plots the current flowing in the input waveguide at the

receiver end of the device as a function of time. In the simulation, we have assumed that both the applied bias and the magnetic field may be switched on a time scale of picoseconds. Further, we also assume that using a hold time of 3 ns gives enough time for the mode to propagate from the sender to the receiver. We can see that the spin polarized current values do not differ much

5 from the non-polarized values, thereby giving an eavesdropper very little additional information as to the value of \underline{b} . Fig. 9 (d) plots the current flowing in the output waveguide at the receiver end of the device as a function of time. While at the I11 maximum the current in the output waveguide does not vanish, the transmission probabilities and, therefore, the current is greatly reduced. While it is ideal for I12 to disappear at the I11 maximum, the device operation, due to

10 the definition of the protocol, is not affected.

The encrypting protocol chosen is a variation of the B92 protocol of C. H. Bennett, cited above. It operates in the following manner. The sender randomly chooses numbers \underline{a} and \underline{b} where \underline{a} corresponds to the location of the density, '0' or '1', and \underline{b} corresponds to the polarization of the propagating density, '0' or '1'. Thus, as the electron density passes the input end of the

15 device into the tunnel region, there are four possible states for the electrons:

$$\psi = \frac{|\psi \uparrow\rangle + |\psi \downarrow\rangle}{\sqrt{2}} \text{ (} a = 0, b = 0\text{)}, |\psi \downarrow\rangle \text{ (} a = 0, b = 1\text{)}, \frac{|\psi \uparrow\rangle + |\psi \downarrow\rangle}{\sqrt{2}} \text{ (} a = 1, b = 0\text{)}, \text{ or } |\psi \downarrow\rangle \text{ (} a = 1, b = 1\text{)}.$$

The receiver then chooses a measurement basis and records the outcome of his or her measurement, his or her measurement basis, and the waveguide in which the electron density arrived. The measurement basis and the waveguide in which the electron density arrived are then publicly communicated to the sender from the receiver to reconcile and throw away

20 incorrect measurements on the arriving density. With a protocol in place, the system is broken up into three operational areas to explain the operation of the device. These are input region, public region, and output region as shown in Fig. 7.

25 The input end of the device is defined as the section of the system that is to the left of the start of the coupling tunnel region 36 in Figs. 1 - 3. It is assumed that the mode that is propagating at the input end of the device consists of mixed spins, or

$$\psi = \frac{|\alpha \uparrow\rangle + |\beta \downarrow\rangle}{\sqrt{2}}$$

where α and β are real numbers. For a message to be sent, the sender varies the electrical or magnetic bias applied to the system at 42, 44 or 52 and the magnetic field applied to the QPC 60. The applied bias is used to control in which waveguide 26 or 32 the electron density arrives at the output end of the device and ultimately determines the value of \underline{a} . Lower biases are used to 5 send the electron density to the output of the input waveguide 26 ($\underline{a} = 0$) and higher biases are used to send the electron density to the output of the output waveguide 32 ($\underline{a} = 1$). This varying of the position of the electron density provides the sender with one basis upon which he or she may send his or her bits. To have a cryptographical key, at least two nonorthogonal bases must be present in the system. As described previously the QPC 60 with a magnetic field applied at 10 64 to polarize the electron spins of the incoming mode that ultimately determines the value of \underline{b} which is the second nonorthogonal basis available to the sender. A high value of magnetic field will polarize the density when $\underline{a} = 0$ and a low magnetic field polarizes the density when $\underline{a} = 1$.

At the input end of the device, the sender controls the operation of the QPC 60 and the electrical or magnetic bias that is applied to the system and the values of these are known only by 15 the sender. Therefore, at the input end the sender may choose to send any of the four states based on the values of the applied bias as illustrated in Fig. 8 and the local magnetic field in the QPC as illustrated in Fig. 9.

As the mode passes through the QPC 60 and assumes one of the four possible states, it enters the public region of the device, which consists of the 335 nm coupling region 36 between 20 the input and output waveguides 26 and 32. In this region, the system is open to eavesdropping from third parties. Nevertheless, this is a rather futile task in that not only must the third party choose one of the four possible bases in which to measure the transmitted bit, but while the electron density interacts with the output waveguide it has not yet revealed its final destination of the input or the output waveguide thereby yielding the eavesdropper no insight as to which basis 25 to choose. This makes the deciphering of the key extremely difficult as the probability of choosing the correct basis is remote. Further, the detection of the eavesdropper is quite simple as the measurement made in the public section of the system, no matter how non-intrusive, will corrupt the transmission coefficients by forcing the wavefunction into a state that does not correspond to the intended state resulting in bit transmission errors detectable by the receiver.

30 With the mode passing the public area of the system, it enters the output end of the device. The output end of the device consists of the 35 nm input and 45 nm section of output

waveguides 26 and 32. As the electron density arrives in either the input or the output waveguide with its given spin polarization, the receiver chooses a value for b by measuring either the input or output waveguide. At the same time, the receiver must also set up the measurement instrumentation to measure either the mixed electron spin of the nonpolarized basis or the spin 5 polarized basis to determine the value of b from the eigenstate of the measurement basis. It should be noted that in the output region, we do not need to assume that we are free from eavesdropping. This is true because the wavefunction is still in one of the four possible states as in the public section of the device. Therefore, the chances of the key being deciphered are still quite low. Once the basis has been chosen and the current is measured, the receiver records the 10 waveguide in which the electron density has arrived, the basis in which the measurement has been made, and the result of the measurement. Information is publicly reconciled and thus, at the end of the reconciliation, the sender and the receiver have the same bit set and the message has been successfully transmitted. If, however, eavesdropping has occurred in either the public or the output region, then discrepancies will show up in the bits measured with the bits sent and 15 the message must be resent.

Although preferred embodiments of the invention have been described in detail, it will be readily appreciated by those skilled in the art that further modifications, alterations and additions to the invention embodiments disclosed may be made without departure from the spirit and scope of the invention as set forth in the appended claims.